UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,532	07/14/2001	Antony John Rogers	063170.6291	3485

5073 7590 11/20/2006

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER
PYZOCHA, MICHAEL J

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 11/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/905,532	**Applicant(s)** ROGERS ET AL.	
	Examiner Michael Pyzocha	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 October 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4,8-16 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,8-16 and 20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08).
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1, 4, 8-16, and 20 are pending.

2. Amendment filed 10/17/2006 has been received and considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 4 and 10-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Chambers, U.S. Patent No. 5,398,196.

As per claims 1, 10, 11, 12, and 14, Chambers discloses a method of detecting viral code in subject files, comprising: creating an artificial memory region spanning one or more components of the operating system (Col 7, line 63 to Col 8, line 21; Col 7, lines 23-28); creating a custom version of an export table, wherein the custom version of the export table is associated with a plurality of entry points and wherein the entry points comprise predetermined values (Col 9, lines 13-32); emulating execution of at least a portion of computer executable code in a subject file (Col 3, lines 42-45); monitoring accesses by the emulated computer executable code to the artificial memory region to detect looping in the execution of the emulated computer executable code (Col 3, lines 51-53; Col 3, line 64 to Col 4, line 14; Col 10 lines 32-50); determining based on a detection of looping whether the emulated computer executable code is viral (Col 3, lines 51-53; Col 3, line 64 to Col 4, line 14; Col 10 lines 32-50).

As per claims 4 and 16, Chambers discloses emulating functionality of the identified operating system call while monitoring the operating system call to determine whether the computer executable code is viral (Col 9, lines 13-25; Col 9, lines 44-54);

As per claims 13 and 15, Chambers discloses a fourth segment comprising auxiliary code, wherein the auxiliary code determines an operating system call that the emulated computer executable code attempted to access (Col 9, lines 13-25; Col 9, lines 44-54); a fifth segment comprising analyzer code, wherein the analyzer code monitors the operating system call to determine whether the computer executable code is viral, while emulation continues (Col 9, lines 13-25; Col 9, lines 44-54);

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 8, 9, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chambers as applied to claims 1 and 14 above, in further view of Golan, U.S. Patent No. 5,974,549.

As per claim 8, Chambers fails to disclose monitoring access by the emulated computer executable code to dynamically linked functions.

However, Golan teaches monitoring access by the emulated computer executable code to dynamically linked functions (Col 6, lines 6-12; Col 5, lines 60-63); and Golan describes a security monitor method whereby access to dynamically linked functions is regulated because, as Golan discloses, "in an operating system that supports virtual memory and hardware abstraction, a software component can only breach security by calling a system call" (Col 5, lines 38-41).

It would have been obvious to one of ordinary skill in that art at the time the invention was filed to have combined the teachings of Chambers with those of Golan and monitor access to dynamically linked functions because requesting access to dynamically linked functions could be an attempt to breach security.

As per claim 9, the applicant discloses the method of claim 8, which is met by Chambers in further view of Golan (see above), with the following limitation which is met by Golan:

Wherein the artificial memory region spans a jump table containing pointers to the dynamically linked functions (Col 7, lines 31-35).

Chambers in further view of Golan describes all the limitations of claim 8. Golan describes the additional limitation of a jump table containing pointers to the dynamically linked functions. The jump table is often incorporated with dynamically linked functions to store the actual addresses of the dynamically linked functions. It would have been obvious to one of ordinary skill in the art at the time in the invention was filed to have included a jump table with the method so that there could be a way of storing the actual addresses of the dynamically linked functions.

As per claim 20, the applicant discloses the method of claim 14, which is met by Chambers (see above), with the following limitation which is met by Golan:

Wherein the artificial memory region created by the memory manager component spans a jump table containing pointers to dynamically linked functions, and the monitor component monitors access by the emulated computer executable code to the dynamically linked functions.

The claim is met by the combination of claims 8 and 9. Explanations for claim 8 and 9 rejections are listed above.

Response to Arguments

6. Applicant's arguments filed 10/17/2006 have been fully considered but they are not persuasive. Applicant argues Chambers fails to the looping as claimed in each independent claim and that Golan fails to teach monitoring access to dynamically linked functions.

With respect to Applicant's argument that Chambers fails to disclose looping, Applicant is directed to column 3 line 64 through column 4 line 14 and column 10 lines 32-50. Where as Applicant admits Chambers teaches repeating a process to determine the results as to whether something is a virus. Since Applicant's specification provides no definition as to what "looping" specifically means Examiner has relied upon the definition of "loop", taken from the Microsoft Computer Dictionary, "A set of statements in a program executed repeatedly, either a fixed number of times or until some condition is true or false”. Based on the cited portions of Chambers, the emulation process is repeated and stopped when a first guinea pig file passes modification behavior (which was passed to it from the original) onto a second guinea pig file and the repeating is stopped after identifying this second passing of modification behavior as described in column 10 lines 40-50. Since the passing of modification behavior is being repeated based on the repeated emulations and the passing of this behavior is an indication that the process is viral; Chambers teaches looping and detection of a virus based on looping.

With respect to Applicant’s argument that Golan fails to teach monitoring access to dynamically linked functions, Golan teaches monitoring access to API functions and the API functions call DLLs (see column 7 lines 23-41). When Golan teaches monitoring API functions, Golan teaches monitoring calls to DLLs and therefore teaches monitoring access to DLLs (i.e. dynamically linked functions).

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Nachenberg (US 6971019) and Wells (US 6338141) teach monitoring for loops to indicate a virus.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

EMMANUEL L. MOISE
SUPERVIS EXAMINER